บทที่ 13

จริยธรรมและความปลอดภัย

บทที่ 13 จริยธรรมและความปลอดภัย

- **ความหมายของจริยธรรม**
  - แบบแผนความประพฤติ หรือความมีสามัญสำนึกต่อสังคมในทางที่ดี
  - ไม่มีกฎเกณฑ์ตายตัวขึ้นอยู่กับกลุ่มสังคมหรือการยอมรับในสังคมนั้นเป็นหลัก
  - เกี่ยวข้องกับการคิดและตัดสินใจได้ว่าสิ่งไหน ควร-ไม่ควร ดี-ไม่ดี ถูก-ผิด

จริยธรรมกับกฎระเบียบ

- **“มีจริยธรรม”** มีสามัญสำนึกดี ประพฤติปฏิบัติดี ไม่ก่อให้เกิดผลเสียหายต่อสังคมโดยรวม
- **“ขาดจริยธรรม”** มีรูปแบบการประพฤติหรือปฏิบัติตนที่ไม่มีประโยชน์หรืออาจส่งผลไม่ดีต่อสังคม
- การควบคุมให้คนมีจริยธรรมที่ดี อาจใช้ข้อบังคับ กฎ หรือระเบียบของสังคมมาเป็นส่วนสนับสนุนให้เกิด “จริยธรรมที่ดี” ได้

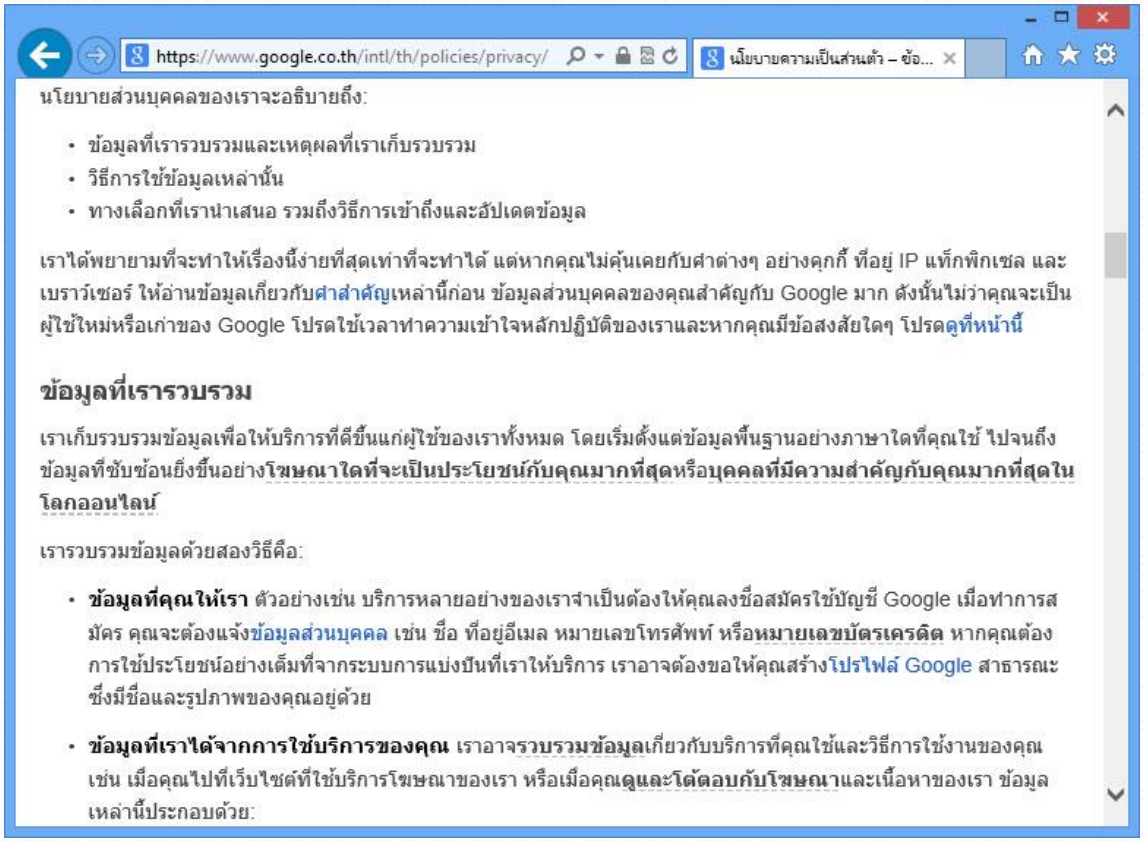
จริยธรรมกับสังคมยุคสารสนเทศ

- ตั้งอยู่บนพื้นฐาน 4 ประเด็นคือ
  - ความเป็นส่วนตัว (Information Privacy)
  - ความถูกต้องแม่นยำ (Information Accuracy)
  - ความเป็นเจ้าของ (Information Property)
  - การเข้าถึงข้อมูล (Information Accessibility)

ความเป็นส่วนตัว (Information Privacy)

- ความเป็นส่วนตัว หมายถึง สิทธิส่วนตัวของบุคคล หน่วยงาน หรือองค์กร ที่จะคงไว้ซึ่งสารสนเทศที่มีอยู่นั้น เพื่อตัดสินใจได้ว่าจะสามารถเปิดเผยให้ผู้อื่นนำไปใช้ประโยชน์ต่อหรือเผยแพร่ได้หรือไม่
- การละเมิดความเป็นส่วนตัว เช่น
  - ใช้โปรแกรมติดตามและพฤติกรรมผู้ที่ใช้งานบนเว็บไซต์
  - การเอาฐานข้อมูลส่วนตัว รวมถึงอีเมล์ของสมาชิกส่งไปให้กับบริษัทผู้รับทำโฆษณา
  - ฯลฯ

ความเป็นส่วนตัว (ต่อ)



คำชี้แจงสิทธิส่วนบุคคลก่อนใช้บริการ

ความเป็นส่วนตัว (ต่อ)

- **ความเป็นส่วนตัวในยุคสังคมออนไลน์** (Social Network)
  - เจ้าของข้อมูลตั้งใจเปิดเผยเรื่องราวส่วนตัวเอง
  - ความเป็นส่วนตัวในยุคของเครือข่ายสังคมออนไลน์ถูกมองข้ามไปมาก
  - เหตุการณ์หรือกิจกรรมต่างๆถูกเปิดเผยแทบตลอดเวลา
  - ผู้ไม่ประสงค์ดีอาจคอยติดตามข้อมูลข่าวสารของเราได้
  - อาจเกิดอันตรายต่อทรัพย์สินและความมั่นคงของชีวิตได้

ความถูกต้องแม่นยำ (ต่อ)

- สารสนเทศที่นำเสนอ ควรเป็นข้อมูลที่มีการกลั่นกรองและตรวจสอบความถูกต้อง และสามารถนำเอาไปใช้ประโยชน์ได้ โดยไม่ส่งผลกระทบกับผู้ใช้งาน
- ตัวอย่างเช่น แหล่งข่าวทางอินเทอร์เน็ต อาจนำเสนอเนื้อหาที่ไม่ได้กลั่นกรอง เมื่อนำไปตีความและเข้าใจว่าเป็นจริง จะทำให้เกิดความผิดพลาดได้
- ผู้ใช้งานสารสนเทศควรเลือกรับข้อมูลจากแหล่งที่น่าเชื่อถือ และตรวจสอบที่มาได้

ความถูกต้องแม่นยำ (ต่อ)

▲ ตัวอย่างข้อมูลที่แชร์ต่อกันไปทางอินเทอร์เน็ต

กรมวิทยาศาสตร์การแพทย์ โต้ข่าวลือยัน น้ำขวดพลาสติกเก็บในรถนานๆ ไม่ก่อสารพิษ ดื่มได้ หลังทดสอบไม่พบสารก่อมะเร็งตามข่าวในโลกออนไลน์

รายงานข่าวแจ้งว่า วานนี้ (2 มิ.ย. 57) กรมวิทยาศาสตร์การแพทย์ กระทรวงสาธารณสุข (สธ.) นำโดย นพ.อภิชัย มงคล อธิบดี ได้ออกมาเปิดเผยข้อมูล หลังมีข่าวลือในโลกออนไลน์ว่า การดื่มน้ำบรรจุขวดพลาสติกที่เก็บในหลังรถยนต์และจอดแช่กลางแดดนานๆ เสี่ยงต่อการเป็นโรคมะเร็งเต้านม และมะเร็งอื่นๆ เนื่องจากแสงแดดจะไปทำปฏิกิริยากับขวดพลาสติก จนเกิดมีสารไดออกซินปะปนมาด้วยนั้น ว่า

ยังไม่มีหลักฐานทางวิทยาศาสตร์ยืนยันตรวจพบไดออกซินในพลาสติก และสารเคมีต่าง ๆ ละลายออกมาจากขวดพลาสติก ทั้งในสภาวะอุณหภูมิสูง หรือสภาวะการแช่แข็ง และจากการทดลองได้ผลยืนยันว่า ไม่พบสารประกอบกลุ่มไดออกซิน และพีซีบีละลายออกมาในทุกตัวอย่าง ดังนั้นจึงอยากเตือนผู้บริโภคควรพิจารณาแหล่งของข่าวสารต่างๆ ที่ได้รับจากสื่อสังคมออนไลน์และตรวจสอบที่มาด้วยเพื่อให้ได้ข้อมูลที่ถูกต้องน่าเชื่อถือ

สำหรับ สารไดออกซิน (Dioxins) เป็นผลผลิตทางเคมีที่เกิดขึ้นโดยมิได้ตั้งใจ จากการเผาไหม้ที่ไม่สมบูรณ์และกระบวนการเผาไหม้อุณหภูมิสูงทุกชนิด โดยมีแหล่งกำเนิดสำคัญของสารกลุ่มนี้คือกระบวนการผลิตเคมีภัณฑ์ที่มีสารคลอรีนเป็นองค์ประกอบ ซึ่งแม้ว่าขวดพลาสติกบางชนิดจะมีส่วนผสมของสารคลอรีน แต่อุณหภูมิของน้ำในขวดที่ถูกวางไว้หลังรถไม่ได้สูงมากพอที่จะทำให้เกิดสารไดออกซินขึ้นมาได้ และขวดชนิดดังกล่าวก็ไม่นิยมนำมาบรรจุน้ำสำหรับดื่มเช่นกัน

▲ ข่าวที่ออกมาชี้แจงความถูกต้องของเนื้อหาที่แชร์กัน

ความเป็นเจ้าของ (Information Property)

- สังคมยุคสารสนเทศมีการเผยแพร่ข้อมูลอย่างง่ายดาย มีเครื่องมือและอุปกรณ์สนับสนุนมากขึ้น
- ก่อให้เกิดการลอกเลียนแบบ ทำซ้ำ หรือละเมิดลิขสิทธิ์ (Copyright) โดยเจ้าของผลงานได้รับผลกระทบทั้งทางตรงและทางอ้อม
- ตัวอย่างเช่น การทำซ้ำหรือผลิตซีดีเพลง และโปรแกรมละเมิดลิขสิทธิ์

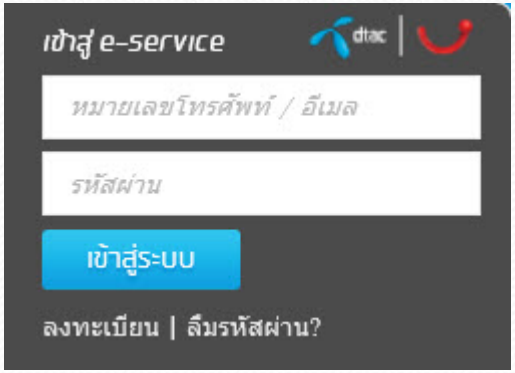
ความเป็นเจ้าของ (ต่อ)

การแสดงความเป็นเจ้าของข้อมูลบนเว็บไซต์ของผู้ให้บริการ

ความเป็นเจ้าของ (ต่อ)

- **การอนุญาตให้ใช้งาน** (License)
  - Copyright  หากมีข้อความนี้จะหมายถึงสงวนลิขสิทธิ์ ห้ามนำเอาผลงานไปใช้หรือทำซ้ำโดยเด็ดขาด นอกจากมีการขออนุญาตอย่างเป็นทางการจากเจ้าของผลงานก่อน
  - Creative Commons  หรือเรียกว่า Copyleft  (เพื่อให้สอดคล้องกับคำว่า Copyright) เป็นการอนุญาตให้นำผลงานไปใช้ต่อยอดได้ในบางกรณี
  - Public Domain  เป็นผลงานที่ไม่สงวนลิขสิทธิ์ จะนำไปใช้งานอะไรก็ได้ แต่ในทางปฏิบัติควรให้เครดิตเจ้าของผลงานกำกับไว้ด้วยเสมอ

การเข้าถึงข้อมูล (Information Accessibility)



- ผู้ดูแลระบบ จะเป็นผู้ที่กำหนดสิทธิ์ในการเข้าถึงข้อมูลของผู้ใช้แต่ละคน เช่น เข้าถึงข้อมูลโดยชื่อผู้ใช้ (Username) และรหัสผ่าน (Password)
- การเข้าถึงข้อมูลนั้นสามารถให้บริการและเข้าถึงได้หลากหลายวิธี เช่น
  - ภาพถ่ายหรือรูปภาพที่ปรากฏบนเว็บไซต์ ควรมีคำอธิบายภาพ (Attribute หรือ Alt) เพื่อสื่อความหมายไว้ด้วยว่าเป็นภาพอะไร
  - สร้างชื่อลิงก์ (Link) ที่มีความหมายในตัว เพื่อบอกให้ผู้ใช้ทราบ

การเข้าถึงข้อมูล (Information Accessibility) (ต่อ)

- **ระบบล็อคสองขั้นตอน** (Two-Step Verification)
  - บางระบบมีบริการ *“ล็อคสองขั้นตอน”* เพื่อป้องกันผู้ไม่หวังดีแอบล็อกอินเข้าใช้บัญชีส่วนตัว
  - ตัวอย่างเช่น *บัญชี Gmail* ของ Google หรือ *บัญชี Appple ID* บนสมาร์ทโฟนระบบ iOS โดยจะผูกเบอร์โทรศัพท์ไว้กับบัญชีอีเมล์
  - ถ้ามีการล็อกอินเข้าระบบจากคอมพิวเตอร์ หรืออุปกรณ์เครื่องอื่นที่เราไม่เคยใช้ ระบบจะส่ง SMS แจ้งรหัสพิเศษมายังโทรศัพท์

การเข้าถึงข้อมูล (Information Accessibility) (ต่อ)

▲ https://appleid.apple.com

▲ https://accounts.google.com/SMSAuthConfig

อาชญากรรมคอมพิวเตอร์ (Computer Crime)

- การลักลอบนำเอาข้อมูลไปใช้โดยไม่ได้รับอนุญาต รวมถึงการสร้างความเสียหายต่อบุคคลและสังคมโดย “ผู้ไม่ประสงค์ดี” เกิดขึ้นจากการขาด “จริยธรรมที่ดี”
- บางกรณีถือว่าเป็นการกระทำที่ผิดกฎหมาย ซึ่งมีบทลงโทษแตกต่างกันไป
- ตัวอย่างของอาชญากรรมคอมพิวเตอร์ เช่น
  - การลักลอบเข้าถึงโดยไม่ได้รับอนุญาต
  - การขโมยและทำลายอุปกรณ์
  - การขโมยโปรแกรมคอมพิวเตอร์
  - การก่อกวนระบบด้วยโปรแกรมประสงค์ร้าย
  - การก่อกวนระบบด้วยสปายแวร์
  - การก่อกวนระบบด้วยสแปมเมล์
  - การหลอกลวงเหยื่อเพื่อล้วงเอาข้อมูลส่วนตัว

การลักลอบเข้าถึงโดยไม่ได้รับอนุญาต

- อาชญากรรมที่เกี่ยวข้องกับการลักลอบหรืออ่านข้อมูลและนำไปใช้โดยไม่ได้รับอนุญาต
- เช่น การลักลอบเข้าไปแก้ไขข้อมูลเว็บเพจหน้าแรกขององค์กร
- กลุ่มคนที่เกี่ยวข้อง เช่น
  - แฮกเกอร์ (Hacker)
  - แครกเกอร์ (Cracker)
  - สคริปต์คิดดี้ (Script Kiddy)

ตัวอย่างการเข้าไปเปลี่ยนแปลงข้อมูลเว็บเพจหน้าแรก แทนที่หน้าเว็บเพจเดิม

การลักลอบเข้าถึงโดยไม่ได้รับอนุญาต (ต่อ)

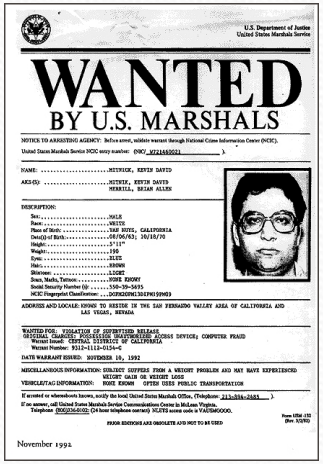
- **แฮกเกอร์** (Hacker)
  - เป็นกลุ่มคนที่มีความรู้ทางด้านคอมพิวเตอร์และระบบเครือข่ายคอมพิวเตอร์เป็นอย่างดี
  - บางคนอาจไม่ได้มีเจตนามุ่งร้ายต่อข้อมูล แต่ทำเพื่อต้องการทดสอบความรู้ของตนเอง นิยมเรียกคนกลุ่มนี้ว่า *คนหมวกขาว* หรือ *White Hat*

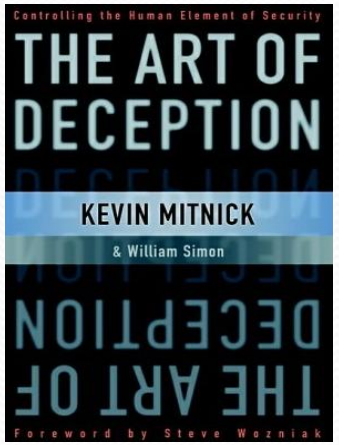
การลักลอบเข้าถึงโดยไม่ได้รับอนุญาต (ต่อ)

- **แครกเกอร์** (Cracker)
  - เป็นกลุ่มคนที่มีความรู้ความสามารถเช่นเดียวกับกลุ่มแฮกเกอร์
  - มุ่งทำลายระบบหรือลักลอบนำเอาข้อมูลนั้นไปแก้ไข เปลี่ยนแปลง หรือทำลายทิ้ง
  - มักเรียกว่าเป็น *กลุ่มคนหมวกดำ* หรือ *Black Hat*
  - มีเจตนาจงใจให้ข้อมูลเกิดความเสียหายมากกว่าแฮกเกอร์

การลักลอบเข้าถึงโดยไม่ได้รับอนุญาต (ต่อ)

- เควิน มิตนิค (Kevin Mitnick)
  - บุคคลที่เป็นทั้งแฮกเกอร์และแครกเกอร์ในคนเดียวกัน
  - ขณะวัยรุ่นได้ใช้ความรู้ของตนเองก่อความเสียหายให้กับหน่วยงานอื่นๆ
  - ปัจจุบันหันมาให้ความรู้เกี่ยวกับระบบรักษาความปลอดภัยบนเครือข่ายแทน





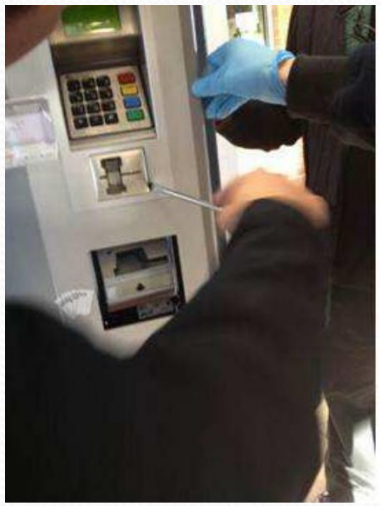
การลักลอบเข้าถึงโดยไม่ได้รับอนุญาต (ต่อ)

- **สคริปต์คิดดี้** (Script Kiddy)
  - มักเป็นคนอยากรู้อยากเห็น ไม่จำเป็นต้องมีความรู้เกี่ยวกับการเจาะเข้าระบบมากนัก
  - มีการแลกเปลี่ยนโปรแกรมหรือสคริปต์ (Scripts) ที่มีคนเขียนและนำออกมาเผยแพร่ให้ทดลองใช้กัน
  - อาศัยโปรแกรมหรือเครื่องมือบางอย่างที่หามาได้ เช่น
    การแฮกอีเมล์ การขโมยรหัสผ่านของผู้อื่น หรือการใช้โปรแกรมก่อกวนอย่างง่าย

การลักลอบเข้าถึงโดยไม่ได้รับอนุญาต (ต่อ)

- **การลักลอบดักข้อมูลด้วยวิธี Skimming** เป็นวิธีการที่ผู้ร้ายใช้โจรกรรมข้อมูล เช่น
  - นำอุปกรณ์อ่านข้อมูลขนาดเล็กไปแอบติดตั้งไว้ตามตู้ ATM เพื่อขโมยรหัส
  - ใช้เครื่อง Skimmer แอบดึงข้อมูลบัตรเครดิต

▲ปุ่มกดปลอมเพื่อแอบเก็บรหัสบัตร ATM



การขโมยและทำลายอุปกรณ์

- เกิดจากการไม่รอบคอบ และวางอุปกรณ์ไว้ในบริเวณที่เสี่ยงต่อการโจรกรรมได้ง่าย
- อาจเกิดจากบุคคลภายนอกหรือภายในองค์กร
- ควรมีการติดตั้งอุปกรณ์ป้องกันและรักษาความปลอดภัย ตรวจการเข้าออกของบุคคลที่มาติดต่อ รวมถึงวางมาตรการในการใช้อุปกรณ์อย่างเข้มงวด

การขโมยโปรแกรมคอมพิวเตอร์

- อาชญากรรมที่เกี่ยวข้องกับการขโมยเอาข้อมูลโปรแกรม รวมถึงการคัดลอกโปรแกรมโดยผิดกฎหมาย
- สามารถทำซ้ำได้ง่าย ก่อให้เกิดความเสียหายกับบริษัทผู้ผลิต
- ลักลอบทำซ้ำข้อมูลโปรแกรม และนำออกวางจำหน่ายแทนที่โปรแกรมต้นฉบับจริง
- กลุ่มผู้ผลิตมีการออกกฎควบคุมการใช้ซอฟต์แวร์ และรวมกลุ่มกันเรียกว่า *BSA (Business Software Alliance)*

การขโมยโปรแกรมคอมพิวเตอร์ (ต่อ)

- **กลุ่ม BSA** (Business Software Alliance)
  - คือกลุ่มพันธมิตรธุรกิจซอฟต์แวร์
  - มีเครือข่ายครอบคลุมอยู่มากกว่า 80 ประเทศทั่วโลก
  - จัดตั้งขึ้นเพื่อควบคุมและดูแลเรื่องการละเมิดลิขสิทธิ์
  - รวมถึงการทำความเข้าใจกับผู้บริโภคให้ตระหนักถึงการใช้งานโปรแกรมที่ถูกต้อง

การก่อกวนระบบด้วยโปรแกรมประสงค์ร้าย

- เป็นการใช้โปรแกรมที่มุ่งเน้นก่อกวนและทำลายระบบข้อมูลคอมพิวเตอร์
- สร้างความเสียหายต่อข้อมูลและระบบคอมพิวเตอร์เป็นอย่างมาก
- กลุ่มโปรแกรมประสงค์ร้ายต่างๆ มีดังนี้
  - ไวรัสคอมพิวเตอร์ (Computer Virus)
  - เวิร์มหรือหนอนอินเทอร์เน็ต (Worm)
  - ม้าโทรจัน (Trojan horses)

การก่อกวนระบบด้วยโปรแกรมประสงค์ร้าย (ต่อ)

- **ไวรัสคอมพิวเตอร์** (Computer Virus)
  - เขียนโดยนักพัฒนาโปรแกรมที่มีความชำนาญเฉพาะด้าน
  - การทำงานจะอาศัยคำสั่งที่เขียนขึ้นภายในตัวโปรแกรมเพื่อกระจายไปยังเครื่องคอมพิวเตอร์เป้าหมาย
  - แพร่กระจายโดยอาศัยคนกระทำการอย่างใดอย่างหนึ่งกับพาหะที่โปรแกรมไวรัสนั้นแฝงตัวอยู่ เช่น รันโปรแกรม อ่านอีเมล์ เปิดดูเว็บเพจ หรือเปิดไฟล์ที่แนบมา

การก่อกวนระบบด้วยโปรแกรมประสงค์ร้าย (ต่อ)

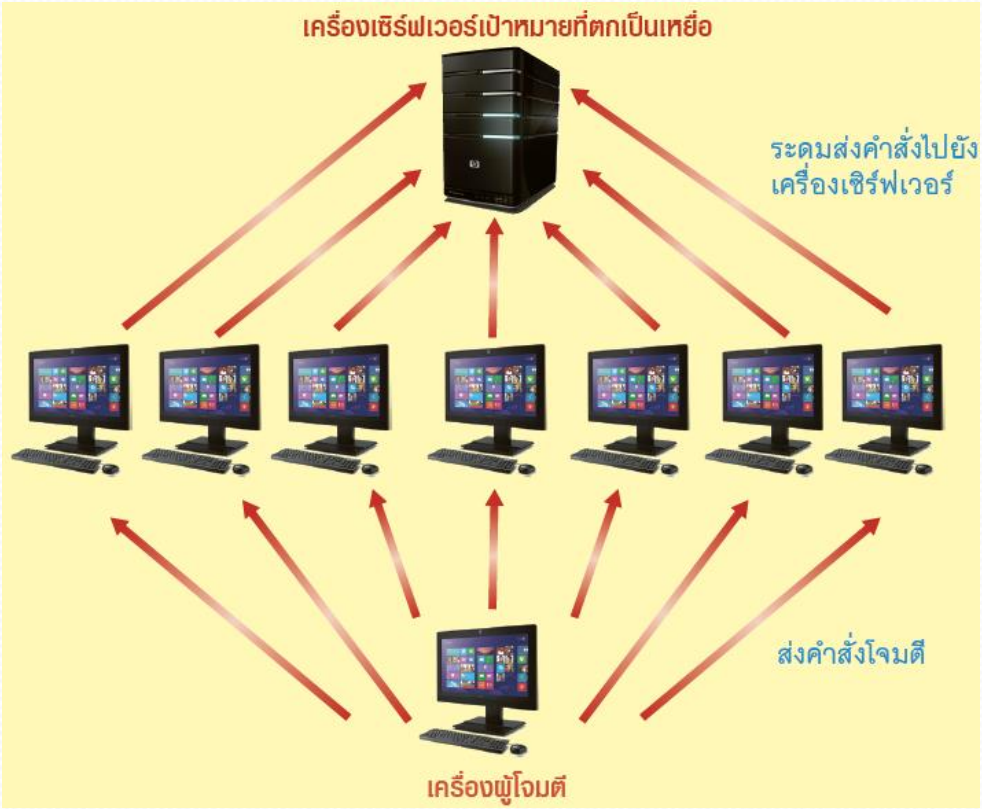
- **เวิร์ม** หรือหนอนอินเทอร์เน็ต (Worm)
  - เป็นโปรแกรมที่มีความรุนแรงกว่าไวรัสคอมพิวเตอร์
  - จะทำลายระบบทรัพยากรคอมพิวเตอร์ให้มีประสิทธิภาพลดลง และไม่อาจทำงานต่อไปได้
  - การทำงานจะตรวจสอบเพื่อโจมตีหาเครื่องเป้าหมายก่อน จากนั้นจะวิ่งเจาะเข้าไปเอง
  - ลักษณะเด่นคือ สามารถทำสำเนาซ้ำตัวเองได้อย่างมหาศาลภายในเวลาเพียงไม่กี่นาที

การก่อกวนระบบด้วยโปรแกรมประสงค์ร้าย (ต่อ)

- **ม้าโทรจัน** (Trojan horses)
  - ทำงานโดยอาศัยการฝังตัวอยู่ในระบบคอมพิวเตอร์เครื่องนั้น และจะไม่แพร่กระจายตัว
  - โปรแกรมจะถูกตั้งเวลาการทำงาน หรือควบคุมการทำงานระยะไกลจากผู้ไม่ประสงค์ดี เพื่อเข้ามาทำงานยังเครื่องคอมพิวเตอร์เป้าหมายได้
  - ตัวอย่างเช่น แสร้งทำเป็นโปรแกรมยูทิลิตี้ให้ใช้งาน แต่แท้จริงคือโปรแกรมอันตราย เมื่อถึงเวลาก็จะทำงานบางอย่างทันที

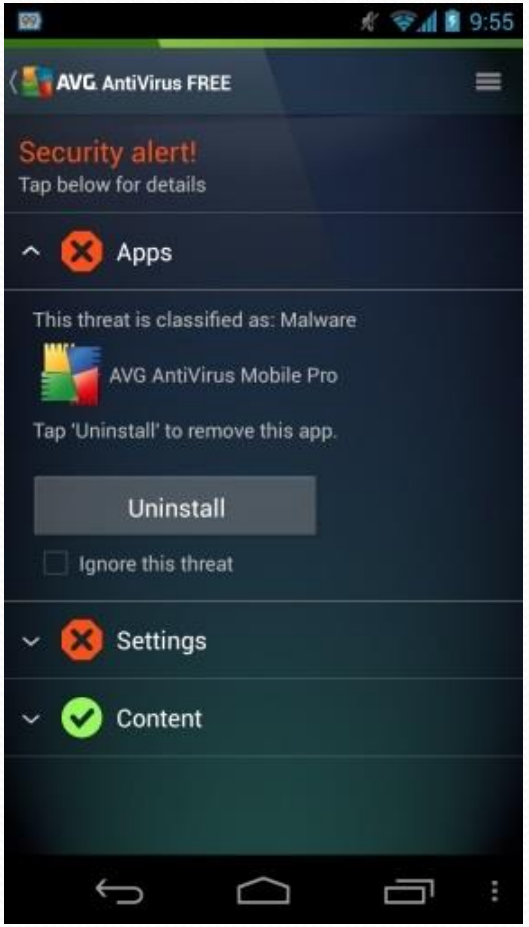
การก่อกวนระบบด้วยโปรแกรมประสงค์ร้าย (ต่อ)

- **ตัวอย่างการโจมตีเครื่องคอมพิวเตอร์ด้วย DoS** (Denial of Service)
  - มุ่งโจมตีเครื่องคอมพิวเตอร์เป้าหมายด้วยการส่งข้อมูลจำนวนมหาศาล เพื่อให้เครื่องดังกล่าวไม่สามารถให้บริการอะไรได้เลย (Denial of Service)
  - เรียกวิธีการโจมตีเหล่านี้ว่า *DoS Attack*



การก่อกวนระบบด้วยโปรแกรมประสงค์ร้าย (ต่อ)

- **ตัวอย่างแอพพลิเคชั่นปลอม/ขยะบนมือถือ**
  - แอพพลิเคชั่นประเภทคีย์บอร์ด ซึ่งคอยดักจับข้อมูลส่วนตัวที่พิมพ์ผ่านคีย์บอร์ด (Keyboard Logger) เช่น Username, Password หรือหมายเลขบัตรเครดิต
  - แอพพลิเคชั่นสแกนไวรัส โดยแจ้งรายละเอียดว่าจะตรวจหาไวรัสบนเครื่อง แต่กลับขโมยข้อมูล SMS บนมือถือเครื่องนั้นส่งไปยังแฮกเกอร์



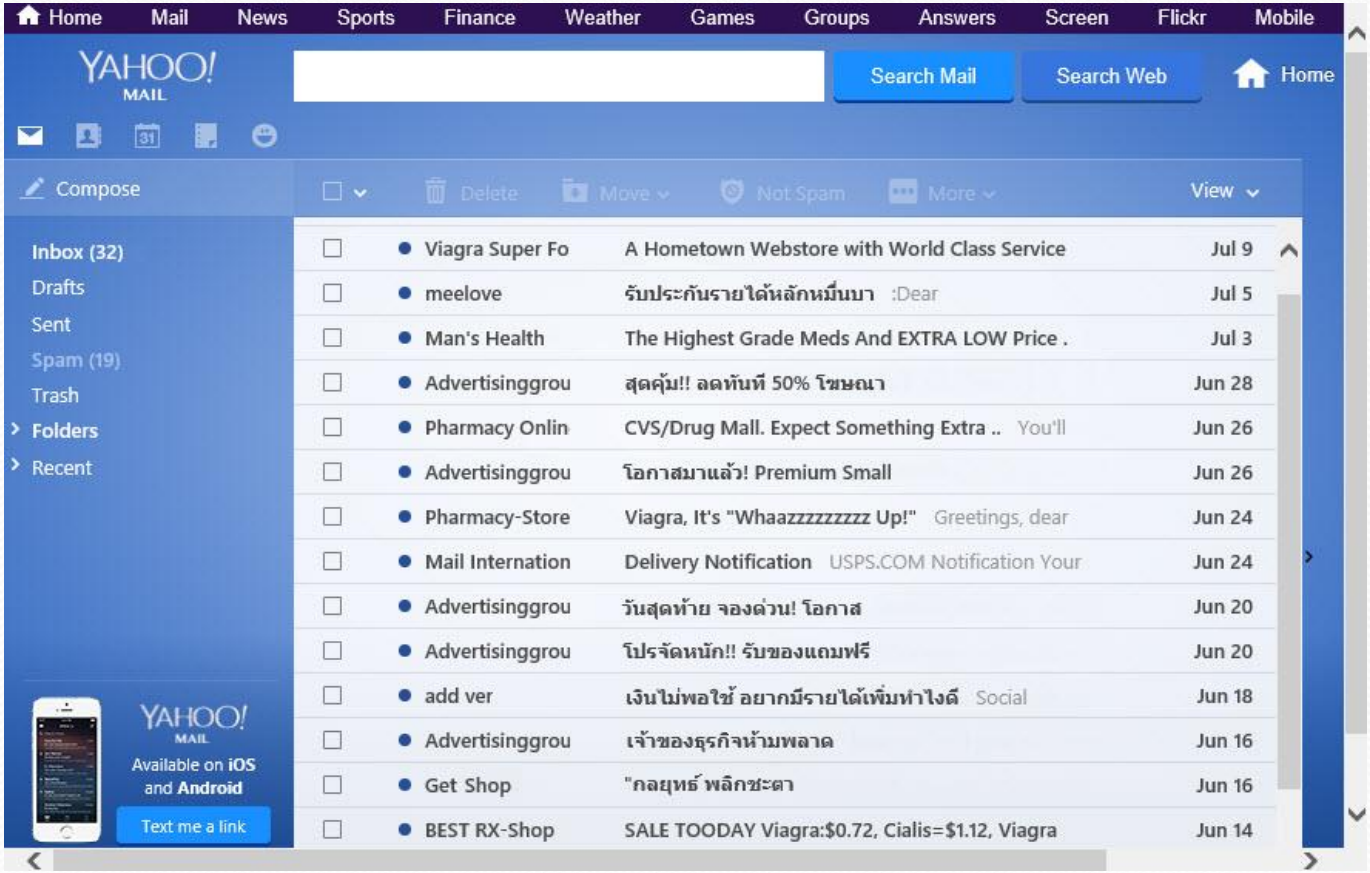
การก่อกวนระบบด้วยสปายแวร์ (Spyware)

- สปายแวร์ เป็นโปรแกรมประเภทสะกดรอยข้อมูล
- ไม่ได้มีความร้ายแรงต่อคอมพิวเตอร์ เพียงแต่อาจทำให้เกิดความน่ารำคาญ
- โดยปกติมักแฝงตัวอยู่กับเว็บไซต์บางประเภท รวมถึงโปรแกรมที่แจกให้ใช้งานฟรีทั้งหลาย
- บางโปรแกรมสามารถควบคุมการเชื่อมต่ออินเทอร์เน็ต แทรกโฆษณาหรือเปลี่ยนหน้าแรกของบราวเซอร์ได้

การก่อกวนระบบด้วยสแปมเมล์ (Spam Mail)

- สแปมเมล์ คือรูปแบบของอีเมล์ที่ผู้รับไม่ต้องการอ่าน
- วิธีการก่อกวนจะอาศัยการส่งอีเมล์แบบหว่านแห และส่งต่อให้กับผู้รับจำนวนมาก
- อาจถูกก่อกวนโดยแฮกเกอร์ หรือเกิดจากการถูกสะกดรอยด้วยโปรแกรมประเภทสปายแวร์
- ส่วนมากเป็นเมล์ประเภทเชิญชวนให้ซื้อสินค้าหรือเลือกใช้บริการของเว็บไซต์นั้นๆ

การก่อกวนระบบด้วยสแปมเมล์ (ต่อ)



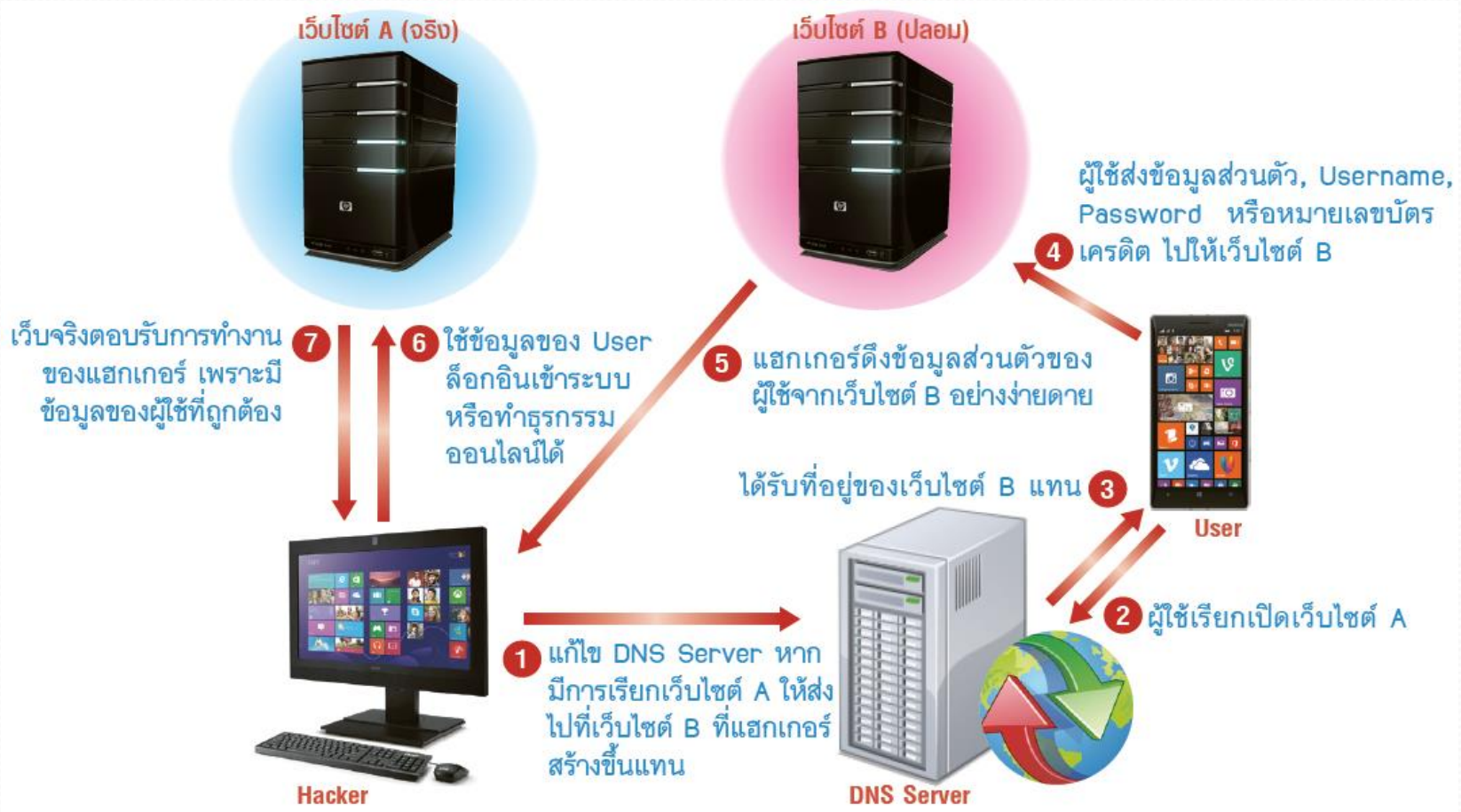
การหลอกลวงเหยื่อเพื่อล้วงเอาข้อมูลส่วนตัว

- เป็นการหลอกลวงเพื่อล้วงข้อมูลส่วนตัว เช่น รายละเอียดหมายเลขบัตรเครดิต ชื่อผู้ใช้ หรือรหัสผ่านสำหรับใช้งานบนเว็บไซต์ โดยใช้กลวิธีต่างๆ เช่น
  - **Phishing** หลอกให้คลิกลิงก์ไปยังเว็บปลอม โดยใช้ข้อความที่เขียนขึ้นมาเอง หลอกลวงให้เหยื่อตายใจและหลงเชื่อกรอกข้อมูลส่วนตัวในเว็บปลอมนั้น
  - **Pharming** เป็นการเข้าโจมตีเซิร์ฟเวอร์ของเว็บไซต์ที่ตกเป็นเหยื่อ เพื่อเปลี่ยนแปลงค่าจากเครื่องเซิร์ฟเวอร์โดยตรง (DNS Hijacking หรือ DNS Redirection) โดยแก้ไขให้ DNS Server ไปเรียกลิงก์ของเว็บปลอมที่ผู้โจมตีสร้างขึ้น เมื่อมีผู้ใช้งานเรียกใช้เว็บไซต์ที่ถูกโจมตี ก็จะถูกส่งต่อไปยังเว็บปลอมโดยไม่รู้ตัว

*** ผู้ใช้งานควรสังเกตชื่อ URL ว่าเรียกไปยังเว็บไซต์ที่ถูกต้อง ก่อนจะกรอกข้อมูลส่วนตัว*

ตัวอย่าง Phishing

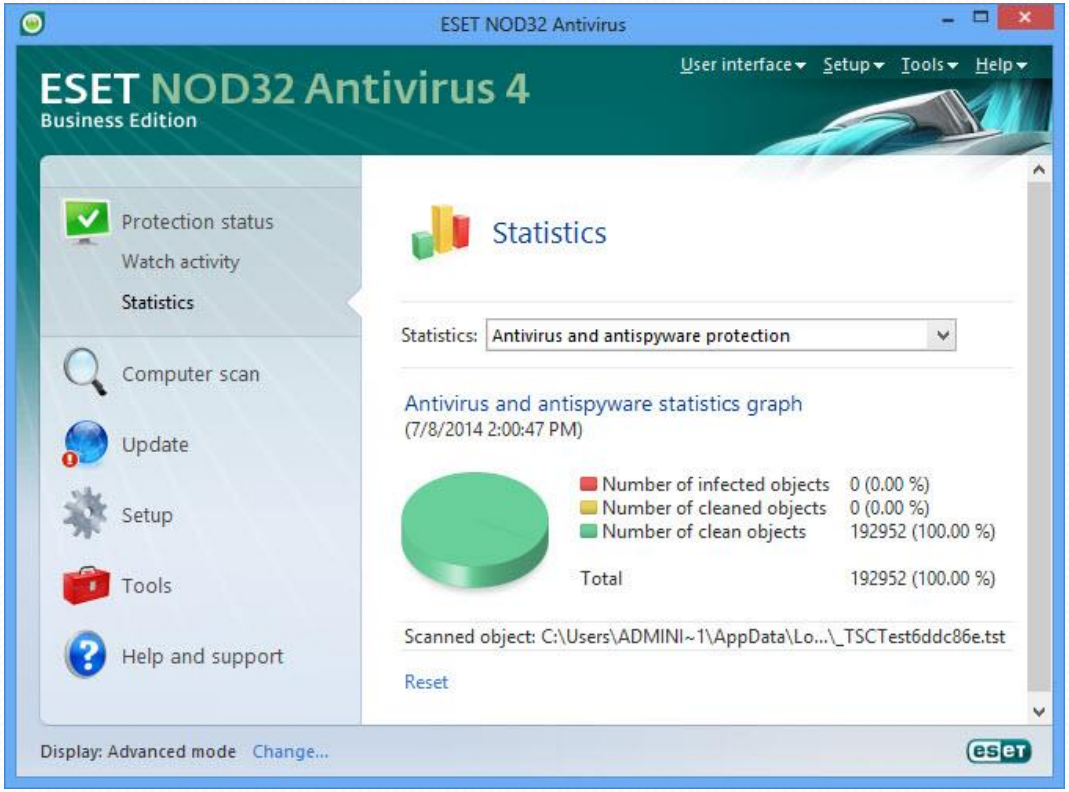
ตัวอย่าง Pharming



การรักษาความปลอดภัยระบบคอมพิวเตอร์

- **การติดตั้งโปรแกรมป้องกันไวรัส** (Antivirus Program)
  - เปรียบเสมือนยามรักษาความปลอดภัยที่มาเฝ้าดูแลบ้าน
  - ทำหน้าที่คอยตรวจสอบและติดตามการบุกรุกของโปรแกรมประสงค์ร้าย เมื่อตรวจพบเจอก็สามารถกำจัดและแจ้งให้ผู้ใช้ทราบได้ทันที
  - ต้องหมั่นอัพเดทโปรแกรมให้มีข้อมูลใหม่ๆอยู่เสมอ เพื่อให้ป้องกันไวรัสได้มีประสิทธิภาพ

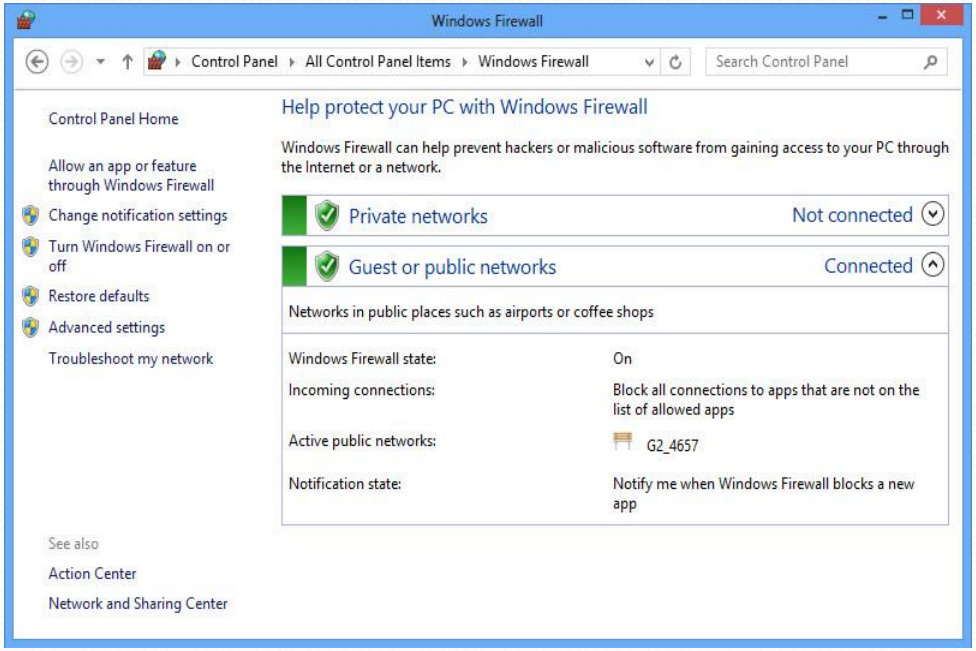
การรักษาความปลอดภัยระบบคอมพิวเตอร์ (ต่อ)



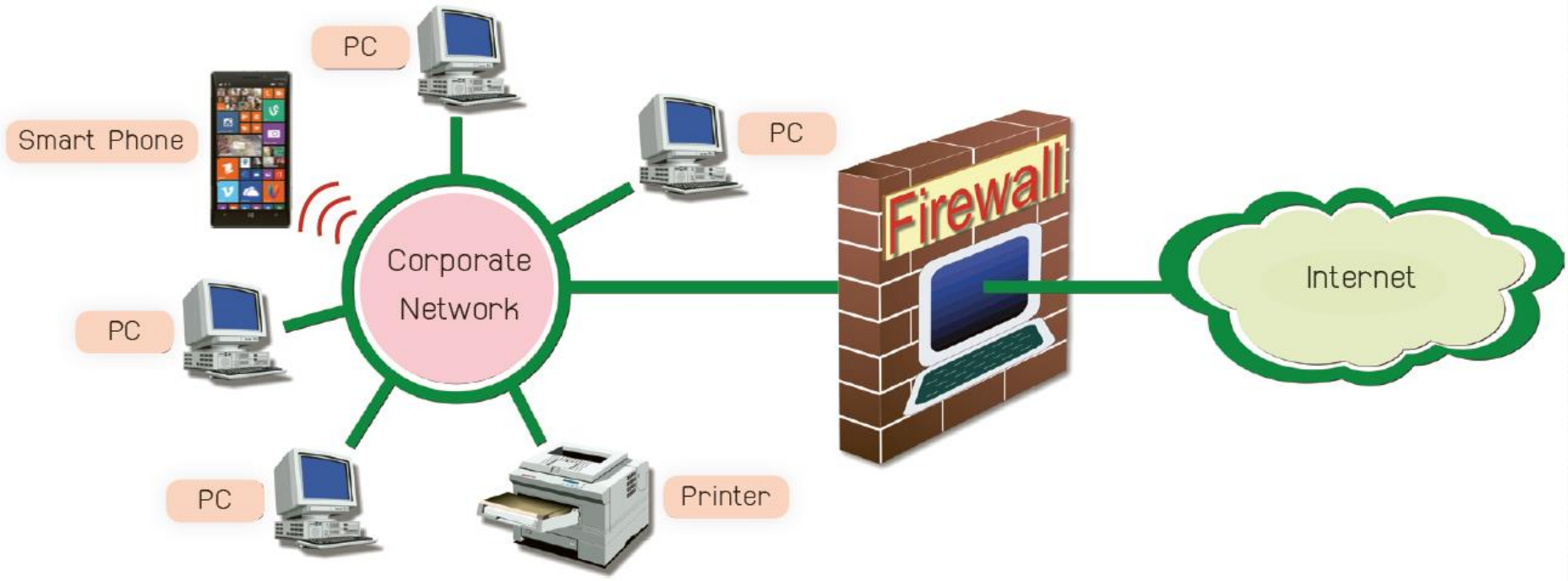
ตัวอย่างโปรแกรมป้องกันไวรัส ESET NOD32 Antivirus

การรักษาความปลอดภัยระบบคอมพิวเตอร์ (ต่อ)

- **การใช้ระบบไฟร์วอลล์** (Firewall System)
  - เป็นระบบรักษาความปลอดภัยที่ประกอบด้วยฮาร์ดแวร์หรือซอฟต์แวร์ก็ได้
  - ทำหน้าที่ดักจับ ป้องกันและตรวจสอบการบุกรุก (Intrusion) เข้าถึงระบบของผู้ไม่ประสงค์ดี
  - ระบบจะให้ข้อมูลเฉพาะที่ได้รับการอนุญาตผ่านเข้าออกเท่านั้น หากไม่ตรงกับเงื่อนไขข้อมูลนั้นจะไม่สามารถผ่านเข้าออกระบบได้



การรักษาความปลอดภัยระบบคอมพิวเตอร์ (ต่อ)

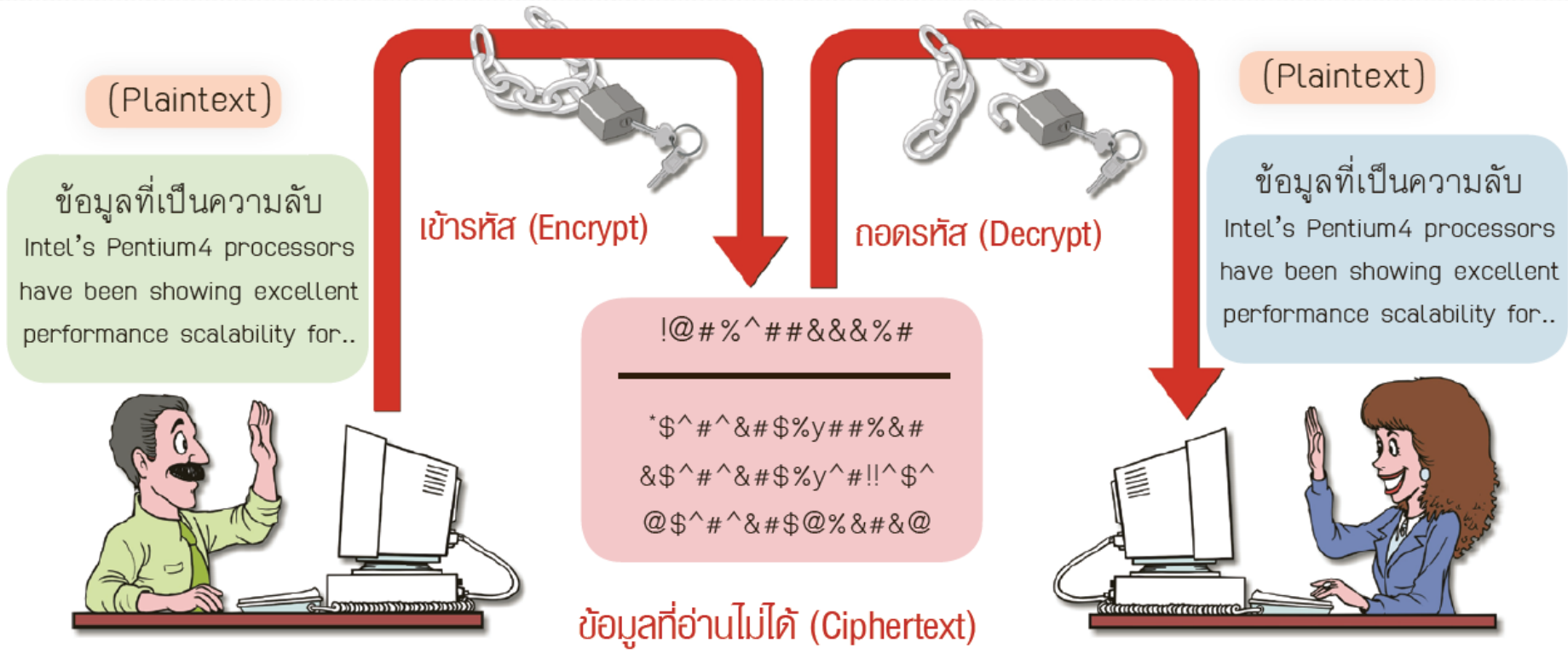


ภาพแสดงการติดตั้งระบบไฟร์วอลล์สำหรับเครือข่าย

การรักษาความปลอดภัยระบบคอมพิวเตอร์ (ต่อ)

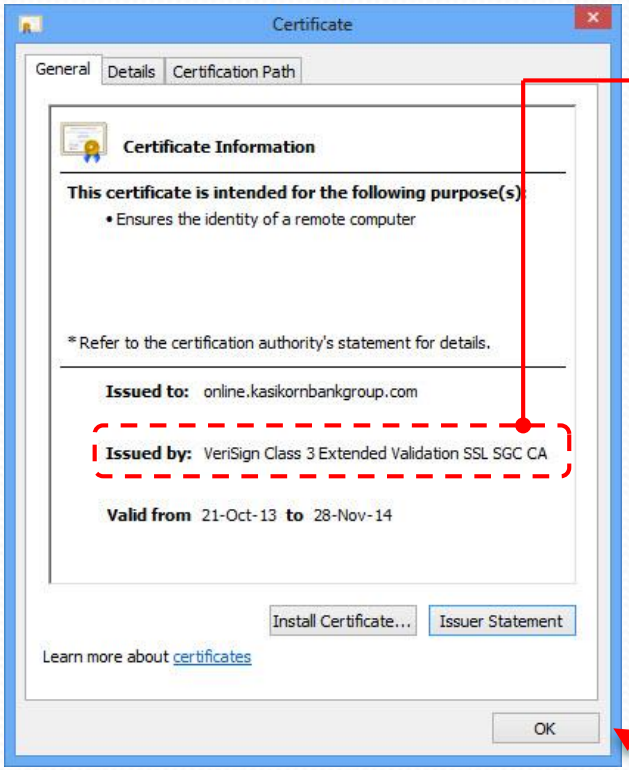
- **การเข้ารหัสข้อมูล** (Encryption)
  - อาศัยสมการทางคณิตศาสตร์ที่ซับซ้อน เพื่อเปลี่ยนแปลงข้อมูลที่อ่านได้ปกติ (Plaintext) ให้ไปอยู่ในรูปแบบที่ไม่สามารถอ่านได้ (Ciphertext)
  - ผู้ไม่ประสงค์ดีที่แอบเอาข้อมูลไปใช้ จะไม่สามารถอ่านข้อมูลที่มีความสำคัญนั้นได้ เพราะมีการเข้ารหัส (Encryption) ไว้
  - การอ่านข้อมูลนั้นจำเป็นต้องถอดรหัสข้อมูล (Decryption) ก่อน โดยใช้กุญแจ (Key) สำหรับไขอ่านข้อมูลนั้นๆ

การรักษาความปลอดภัยระบบคอมพิวเตอร์ (ต่อ)



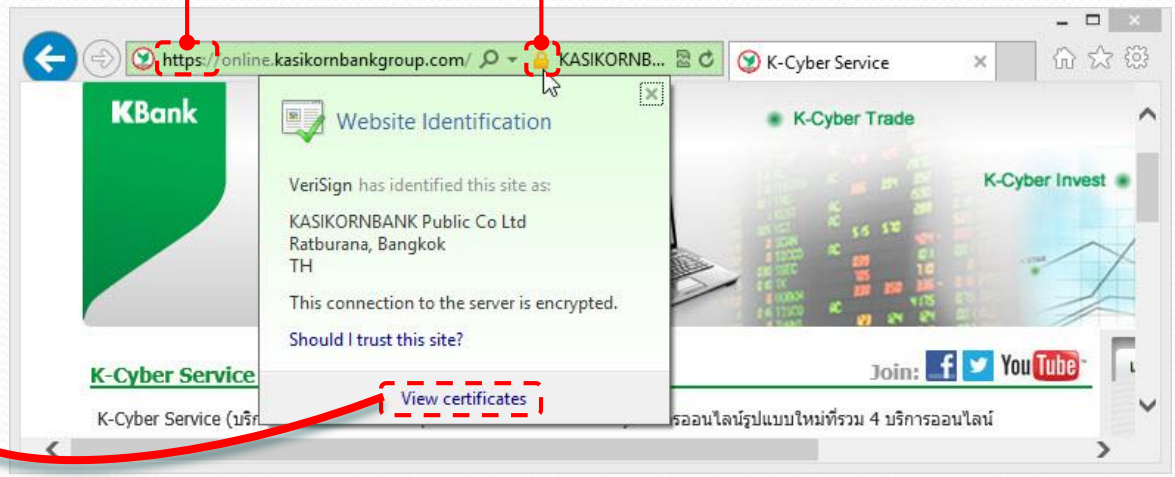
เทคนิคการเข้าและถอดรหัสของข้อมูล

การรักษาความปลอดภัยระบบคอมพิวเตอร์ (ต่อ)



ผู้ออกใบรับรอง (Certificate)

แสดงถึงมีการเข้ารหัสความปลอดภัยบนเว็บนี้



ตัวอย่างหน้าเว็บที่มีการเข้ารหัสเพื่อรักษาความปลอดภัยของข้อมูล

การรักษาความปลอดภัยระบบคอมพิวเตอร์ (ต่อ)

- **การสำรองข้อมูล** (Back up)
  - คือการทำซ้ำข้อมูล ไฟล์ หรือโปรแกรมที่อยู่ในพื้นที่เก็บข้อมูล เพื่อให้สามารถนำกลับมาใช้ได้อีก กรณีที่ข้อมูลต้นฉบับนั้นเกิดสูญหายหรือถูกทำลาย
  - วิธีการสำรองข้อมูลอาจทำทั้งระบบหรือแค่บางส่วน โดยเก็บลงหน่วยเก็บบันทึกข้อมูลสำรอง เช่น ฮาร์ดดิสก์, DVD หรือเทปบันทึกข้อมูล เป็นต้น
  - หากข้อมูลมีความสำคัญมากอาจต้องสำรองข้อมูลทุกวัน หรือทุกสัปดาห์ แต่หากข้อมูลนั้นมีความสำคัญระดับทั่วไป ก็อาจสำรองข้อมูลเป็นรายเดือน

การรักษาความปลอดภัยระบบคอมพิวเตอร์ (ต่อ)

- **ความปลอดภัยบนสื่อสังคมออนไลน์**
  - *ภัยจากการใช้งาน* เช่น ถูกผู้ไม่หวังดีแอบเจาะระบบบัญชี Social Media ของเราแล้วขโมยข้อมูลไปใช้ได้
  - *ภัยทางด้านสังคม* เช่น ถูกหลอกลวงจากคนในสังคมออนไลน์ ทำให้เสียทรัพย์สิน เสียชื่อเสียง เกิดความไม่ปลอดภัยในชีวิต

พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

- ใช้กำหนดมาตรการต่างๆ เพื่อควบคุมและเอาผิดกับผู้กระทำผิดเกี่ยวกับคอมพิวเตอร์ โดยมีผลบังคับใช้ตั้งแต่วันที่ 18 กรกฎาคม 2550 เป็นต้นไป เช่น
  - ทำลาย แก้ไข เปลี่ยนแปลง หรือทำให้ข้อมูลคอมพิวเตอร์ของผู้อื่นเสียหาย
  - เข้าถึงข้อมูลคอมพิวเตอร์ หรือดักรับข้อมูลของผู้อื่นโดยไม่ได้รับอนุญาต
  - ส่งต่ออีเมล์ที่มีข้อมูลไม่เหมาะสม เช่น ภาพ/คลิปหลุดที่ทำให้ผู้อื่นเสื่อมเสีย
  - ส่งข้อมูลรบกวนการใช้ระบบคอมพิวเตอร์ของคนอื่น
  - นำรหัสผ่านของผู้อื่นไปใช้แล้วเกิดความเสียหาย
  - โพสต์ข้อความแสดงความคิดเห็นโดยที่ไม่ไตร่ตรองให้ดี